

Please amend the present application as follows:

Claims

The following is a copy of Applicant's claims that identifies language being added with underlining ("___") and language being deleted with strikethrough ("—"), as is applicable:

1. (Previously presented) A method, comprising:
receiving a user's finger within a finger slot provided in a lid that covers an image window of a scanner of a multifunction peripheral;
obtaining a biometric image of the user's finger by scanning the user's finger with the scanner;
comparing the biometric image to a biometric key; and
authenticating a user of the multifunction peripheral based on a match between the biometric image and the biometric key.
2. (Original) The method of claim 1, additionally comprising distributing storage of each biometric key to a file system of which an originator of the biometric key has control.
3. (Original) The method of claim 1, additionally comprising prompting the user for entry of a user name to direct retrieval of the biometric key.
4. (Original) The method of claim 1, additionally comprising distributing the storage of biometric keys associated with authorized users of the multifunction

peripheral to workstations assigned to the authorized users of the multifunction peripheral, respectively.

5. (Original) The method of claim 1, additionally comprising basing the storage of biometric keys on a server in communication with the multifunction peripheral.

6. (Original) The method of claim 1, additionally comprising basing the storage of biometric keys on the multifunction peripheral.

7. (Original) The method of claim 1, additionally comprising activating the scanner portion of the multifunction peripheral in response to a sensor detecting the user's finger within the finger slot.

8. (Original) The method of claim 1, additionally comprising blocking light from entering the finger slot with a resilient shroud.

9. (Previously presented) A system, comprising:
a multifunction peripheral;
a finger slot that provides access to an image window in a scanner portion of the multifunction peripheral;
a data collection module configured to obtain a biometric image by scanning a user's finger contained within the finger slot using the scanner portion;
a data evaluation module configured to compare the biometric image to a biometric key; and

an authenticator module configured to provide access to the multifunction peripheral based a match between the biometric image and the biometric key.

10. (Original) The system of claim 9, additionally comprising distributed biometric key storage configured to distribute storage of each biometric key within a file system of which an originator of the biometric key has control.

11. (Original) The system of claim 9, additionally comprising a data collection module to prompt the user to enter a user name to direct retrieval of the biometric key from a distributed location.

12. (Original) The system of claim 9, additionally comprising distributed biometric key storage configured to distribute storage of biometric keys associated with authorized users of the multifunction peripheral on workstations assigned to authorized users of the multifunction peripheral, respectively.

13. (Original) The system of claim 9, additionally comprising server based storage of biometric keys, wherein a server upon which the biometric keys are stored is in communication with the multifunction peripheral.

14. (Original) The system of claim 9, additionally comprising multifunction peripheral based storage of biometric keys.

15. (Original) The system of claim 9, additionally comprising a sensor switch adjacent to the finger slot to activate the scanner portion of the multifunction peripheral in response to detection of the user's finger.

16. (Original) The system of claim 9, additionally comprising a shroud within the finger slot.

17. (Currently amended) A ~~processor-readable medium~~ computer-readable medium having processor-readable instructions thereon which, when executed by one or more processors cause the one or more processors to:

obtain a biometric image by scanning with a scanner portion of a multifunction peripheral a finger of a user contained within a finger slot defined within a lid that covers the scanner portion;

compare the biometric image to a biometric key; and

authenticate the user of the multifunction peripheral based on a match between the biometric image and the biometric key.

18. (Currently amended) The A ~~processor-readable media~~ computer-readable medium of claim 17 having processor-readable instructions thereon which, when executed by one or more processors cause the one or more processors to prompt the user for entry of a user name to direct retrieval of the biometric key.

19. (Currently amended) The ~~processor-readable media~~ computer-readable medium of claim 17 having processor-readable instructions thereon which, when executed by one or more processors cause the one or more processors to distribute

storage of each biometric key to a file system over which an originator of the biometric key has control.

20. (Currently amended) The ~~processor-readable media~~ computer-readable medium of claim 17 having processor-readable instructions thereon which, when executed by one or more processors cause the one or more processors to base storage of each biometric key on storage media contained within the multifunction peripheral.

21. (Previously presented) The method of claim 1, further comprising retrieving the biometric key from a remote computer via an encrypted communication.

22. (Previously presented) The system of claim 9, wherein the data evaluation module is configured to retrieve the biometric key from a remote computer via an encrypted communication.

23. (Previously presented) The system of claim 15, wherein the sensor switch comprises an optical or pressure switch.

24. (Currently amended) The ~~processor-readable media~~ computer-readable medium of claim 17 having processor readable-instructions thereon which, when executed by one or more processors cause the one or more processors to retrieve the biometric key from a remote computer via an encrypted communication.

25. (Previously presented) A method for authenticating a user of a peripheral device having a scanner that is used to scan documents, the method comprising:

scanning a potential user's finger using the scanner that is used to scan documents;

obtaining a biometric image of the user's finger from the scanning;

comparing the biometric image to a biometric key; and

authenticating the user if the obtained biometric image matches the biometric key.

26. (Previously presented) The method of claim 25, further comprising receiving the user's finger in a finger slot provided in a lid that covers an image window of the scanner prior to the scanning.

27. (Previously presented) A peripheral device, comprising:

a scanner that is used to scan documents, the scanner including an image window upon which the documents are placed;

a data collection module that is configured to obtain a biometric image of a user finger that is scanned by the scanner when the finger is placed on the image window;

a data evaluation module that is configured to compare the biometric image to a biometric key; and

an authenticator module that is configured to permit the user to use the peripheral device based a match between the biometric image and the biometric key.

28. (Previously presented) The device of claim 27, further comprising a lid that covers the image window of the scanner, the lid including a finger slot that is configured to receive the user finger to enable scanning of the finger.

29. (Previously presented) The device of claim 28, wherein the finger slot includes a shroud that prevents light from entering the finger slot.

30. (Previously presented) The device of claim 28, wherein a sensor switch is provided within the finger slot, the sensor switch being configured to initiate scanning of the user finger when the switch is activated.